BAB I
Pendahuluan

1.1. Latar Belakang

Di era digital yang semakin maju ini, informasi dapat diakses dengan cepat dan mudah oleh banyak orang, sehingga sangat membantu dalam berbagai aspek kehidupan sehari-hari. Internet telah menjadi sumber utama untuk mendapatkan berbagai jenis informasi, baik yang bermanfaat maupun yang kurang bermanfaat. Namun, kemudahan akses tersebut juga menuntut adanya keamanan yang memadai guna melindungi kerahasiaan data dan aktivitas pengguna. Dalam konteks ini, keamanan informasi menjadi krusial untuk mencegah penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab. Perlindungan data sangat penting untuk menjaga privasi pengguna dan menghindari dampak merugikan yang bisa terjadi akibat pelanggaran keamanan.

Perkembangan pesat teknologi digital dan internet di era globalisasi telah menciptakan situasi baru, di mana internet menjadi kebutuhan esensial bagi masyarakat modern. Hampir semua aktivitas sehari-hari, mulai dari komunikasi, pencarian informasi, transaksi digital, hingga hiburan, kini bergantung pada teknologi internet.[1] Penggunaan internet yang luas mempermudah masyarakat dalam mengakses informasi dengan lebih cepat dan efisien. Dalam konteks ini, situs web menjadi salah satu alat utama dalam penyediaan informasi yang mudah dijangkau oleh pengguna dari berbagai latar belakang.

Website atau sering juga disebut sebagai portal atau situs merupakan sebuah platform digital yang dirancang untuk menyajikan informasi dalam berbagai format, seperti teks, gambar, video, dan audio.[2] *Website* bisa bersifat statis di mana kontennya tidak berubah atau dinamis di mana kontennya dapat diperbarui secara berkala sesuai kebutuhan pengguna. Setiap halaman dalam *website* dihubungkan melalui *hyperlink*, yang memungkinkan pengguna untuk berpindah dari satu laman ke laman lainnya dengan mudah. Laman utama atau beranda biasanya menjadi pintu masuk pengguna untuk menjelajahi konten-konten lain yang terdapat dalam *website* tersebut.

Kemajuan teknologi internet tidak hanya memudahkan individu dalam berkomunikasi, tetapi juga mengubah cara institusi publik, seperti pemerintah daerah, berinteraksi dengan masyarakatnya. Pemerintah daerah desa Purwobakti memanfaatkan *website* sebagai sarana utama untuk menjalin komunikasi pengumuman dengan warga desa. Melalui *website*, pemerintah desa dapat memberikan layanan publik secara lebih efisien serta menyebarkan informasi penting secara cepat dan akurat. *Website* ini memainkan peran sentral dalam memfasilitasi interaksi digital antara pemerintah dan masyarakat, sehingga menciptakan pemerintahan yang lebih transparan dan mudah diakses oleh semua lapisan masyarakat.

Meningkatnya penggunaan internet dan ketergantungan pada situs web, muncul juga ancaman keamanan yang semakin kompleks. Risiko kejahatan siber, seperti pencurian data dan peretasan, terus meningkat seiring dengan bertambahnya jumlah pengguna internet. *Website* pemerintah daerah, yang sering kali menyimpan data

penting dan sensitif, menjadi target yang rentan bagi serangan siber. Salah satu ancaman keamanan yang sering mengincar *website* adalah *Cross-Site Scripting* (XSS). Serangan XSS adalah jenis serangan yang memungkinkan penyerang menyisipkan skrip berbahaya (*script*) pada dalam halaman web yang dikunjungi oleh pengguna.[3] Hal ini dapat menyebabkan website daerah rentan terhadap manipulasi, akses tidak sah ke data pengguna, mencuri informasi pribadi, dan bahkan menciptakan situasi dimana pengguna dapat dieksploitasi secara lebih lanjut, yang berpotensi merugikan banyak pihak.

Serangan XSS dapat mengakibatkan website rentan terhadap berbagai jenis manipulasi, termasuk pencurian data pengguna, pengubahan konten, atau bahkan serangan lanjutan yang dapat menyebabkan kerugian lebih besar. Untuk menjaga integritas dan keamanan website, langkah-langkah pencegahan dan mitigasi serangan perlu dilakukan. Salah satu cara yang efektif adalah dengan menerapkan OWASP (*Open Web Application Security Project*) sebagai standar dalam mengevaluasi dan mengidentifikasi celah keamanan yang ada di dalam aplikasi web. OWASP menyediakan berbagai panduan dan alat bantu yang digunakan secara luas untuk melindungi aplikasi web dari berbagai ancaman keamanan, termasuk serangan XSS.

Proses pengidentifikasian celah keamanan menggunakan pendekatan OWASP, yang dikenal sebagai *Vulnerability Assessment* (VA) bertujuan untuk mengidentifikasi potensi kerentanan dan menentukan langkah-langkah perbaikan yang diperlukan. VA adalah proses untuk mengidentifikasi, menganalisis, dan mengklasifikasikan kerentanan keamanan pada sistem, jaringan, aplikasi, atau perangkat keras.[4] Dalam hal ini, VA digunakan untuk memeriksa bagaimana situs web merespons masukan

pengguna dan mengidentifikasi apakah ada celah yang memungkinkan penyisipan skrip berbahaya. Evaluasi ini sangat penting untuk menjaga keamanan data dan informasi yang disajikan di dalam situs web, terutama karena situs tersebut memberikan layanan publik yang vital bagi masyarakat. Dengan mendeteksi kerentanan, langkah-langkah mitigasi yang tepat dapat diambil untuk melindungi situs dari eksploitasi oleh pihak luar.

Dalam penelitian ini, website desa yaitu purwobakti.desa.id untuk menganalisis keamanan terhadap serangan *Cross-Site Scripting* (XSS). Situs web tersebut memuat berbagai informasi penting, seperti berita daerah desa Purwobakti, transparansi anggaran, artikel, pengumuman, peraturan daerah, dan lain-lain. Mengingat pentingnya peran situs web ini, hasil dari penelitian diharapkan dapat memberikan rekomendasi kepada pengelola situs dalam meningkatkan keamanan website, sehingga dapat terus memberikan layanan publik yang aman, andal, dan terpercaya bagi seluruh warga desa.

1.2. Batasan Masalah Penelitian

Agar pengembangan dalam penelitian ini tidak menyimpang dari topik permasalahan yang telah dibentuk, maka ruang lingkup pembahasannya sebagai berikut:

1. Metode yang akan digunakan yaitu mengunakan *Framework Open Worldwide Application Security Project* (OWASP).
2. Parameter analisis masalah mengenai serangan *Cross-Site Scripting* (XSS).

1.3. Rumusan Masalah

Berdasarkan latar belakang masalah, jadi dapat dirumuskan masalah sebagai berikut:

1. Bagaimana menganalisa keamanan website daerah desa Purwobakti menggunakan *Framework Open Worldwide Application Security Project* (OWASP)?
2. Bagaimana tingkat keamanan sebuah website daerah desa Purwobakti dari serangan *Cross-Site Scripting* menggunakan *Framework Open Worldwide Application Security Project* (OWASP)?

1.4. Tujuan Penelitian

Penelitian Analisis Keamanan Informasi Website terhadap Serangan *Cross-Site Scripting*, di lakukan dengan tujuan yaitu:

1. Menganalisa keamanan sebuah website daerah desa Purwobakti agar terhindar dari serangan *Cross-Site Scripting*.
2. Melakukan pengukuran tingkat keamanan website daerah desa Purwobakti dari serangan *Cross-Site Scripting*.

1.5. Manfaat Penelitian

Adapun manfaat yang didapat dari penelitian Analisis Keamanan Website terhadap Serangan *Cross-Site Scripting* sebagai berikut:

1. Mengedukasi pentingnya keamanan sebuah informasi pada website daerah desa Purwobakti.
2. Sebagai referensi tambahan bagi peneliti pada penelitian lain.